

What is claimed is:

1. An encryption evaluation support system,
comprising:

an evaluation executing unit receiving a figure
representation of an encryption algorithm, wherein

5 said figure representation includes a plurality of
unit figures; and

a point storing unit storing points allocated
to said plurality of unit figures respectively, and

10 wherein said evaluation executing unit gives
said points to said plurality of unit figures of said
figure representation, respectively, to output said
points given to said plurality of unit figures of said
figure representation.

2. The encryption evaluation support system
according to Claim 1, wherein said figure
representation is a function block diagram.

3. The encryption evaluation support system
according to Claim 1, wherein said figure
representation is described in a pre-defined
encryption algorithm specification description manner,
5 and

wherein said unit figure is used in said
encryption algorithm specification description manner.

00766675 012004

4. The encryption evaluation support system according to Claim 1, wherein said evaluation executing unit outputs said points to evaluate said encryption algorithm corresponding to said figure representation, before an encryption program is generated based on said encryption algorithm.

5. The encryption evaluation support system according to Claim 1, further comprising:

an automatic replacing unit generating a changed figure representation in which at least one of said plurality of unit figures of said figure representation is automatically replaced by another unit figure, and

wherein said point storing unit stores a point allocated to said another unit figure, and

wherein said evaluation executing unit gives said points to a plurality of unit figures including said another unit figure of said changed figure representation, with reference to said point storing unit, respectively to output said points given to said plurality of unit figures of said changed figure representation.

6. The encryption evaluation support system according to Claim 1, wherein said point storing unit stores said point allocated to said unit figure for

each of a plurality of evaluation items, and

5 wherein said evaluation executing unit gives
said points for selected one of said plurality of
evaluation items to said plurality of unit figures of
said figure representation, respectively, with
reference to said point storing unit to output said
10 points for said selected one given to said plurality
of unit figures of said figure representation.

7. The encryption evaluation support system
according to Claim 6, wherein said plurality of
evaluation items include an evaluation item with
regard to an encryption strength.

8. The encryption evaluation support system
according to Claim 6, wherein said plurality of
evaluation items include an evaluation item with
regard to an estimation of one of a size and a
5 processing amount when said encryption algorithm is
executed in one of a software and a hardware.

9. The encryption evaluation support system
according to Claim 1, wherein said evaluation
executing unit gives said point to one of said
plurality of unit figures of said figure
5 representation, every time a signal flowing in said
figure representation passes through said one of said

09766675.042304

plurality of unit figures of said figure representation.

10. The encryption evaluation support system according to Claim 9, wherein said signal includes a plurality of bits, and

5 wherein said plurality of bits of said signal are passed through said one of said plurality of unit figures in parallel, and

wherein said point storing unit stores said point allocated to said unit figure for each of said plurality of bits, and

10 wherein said evaluation executing unit gives said point for each of said plurality of bits to said unit figure with reference to said point storing unit, to output said point for each of said plurality of bits given to said figure representation.

11. The encryption evaluation support system according to Claim 10, wherein said evaluation executing unit calculates a mean value of said points corresponding to said plurality of bits given to said figure representation, to output.

12. The encryption evaluation support system according to Claim 3, further comprising:

an evaluation target editing unit supporting a

09765675 012304

user who generates said figure representation of said
5 encryption algorithm based on said encryption
algorithm specification description manner.

13. The encryption evaluation support system
according to Claim 1, further comprising:

a result editing unit presenting said points
outputted by said evaluation executing unit in
5 graphical form.

14. The encryption evaluation support system
according to Claim 13, wherein said result editing
unit sorts said points outputted by said evaluation
executing unit to present.

15. The encryption evaluation support system
according to Claim 1, wherein said encryption
algorithm is a type of one of a common key
cryptosystem and a public key cryptosystem.

16. A computer readable recording medium for
recording a program for a process, comprising:

- (a) receiving a figure representation of an
encryption algorithm, wherein said figure
5 representation includes a plurality of unit figures;
(b) storing points allocated to said plurality
of unit figures respectively;

09766675 012304
FOI 2015 0922

(c) giving said points to said plurality of unit figures of said figure representation,
10 respectively; and

(d) outputting said points given to said plurality of unit figures of said figure representation.

17. The computer readable recording medium for recording a program for a process according to Claim 16, wherein said figure representation is described in a pre-defined encryption algorithm specification
5 description manner, and

wherein said unit figure is used in said encryption algorithm specification description manner.

18. The computer readable recording medium for recording a program for a process according to Claim 16, wherein said (d) includes outputting said points to evaluate said encryption algorithm corresponding to
5 said figure representation, before an encryption program is generated based on said encryption algorithm.

19. The computer readable recording medium for recording a program for a process according to Claim 16, further comprising:

(e) generating a changed figure representation

09766675 013301

5 in which at least one of said plurality of unit
figures of said figure representation is automatically
replaced by another unit figure, and

wherein said (b) includes storing a point
allocated to said another unit figure, and

10 wherein said (c) includes giving said points to
a plurality of unit figures including said another
unit figure of said changed figure representation,
respectively, and

wherein said (d) includes outputting said
15 points given to said plurality of unit figures of said
changed figure representation.

20. The computer readable recording medium for
recording a program for a process according to Claim
16, wherein said (b) includes storing said point
allocated to said unit figure for each of a plurality
5 of evaluation items, and

wherein said (c) includes giving said points
for selected one of said plurality of evaluation items
to said plurality of unit figures of said figure
representation, respectively, and

10 wherein said (d) includes outputting said
points for said selected one given to said plurality
of unit figures of said figure representation.

21. The computer readable recording medium for

09766675 012301

recording a program for a process according to Claim
16, wherein said (c) includes giving said point to one
of said plurality of unit figures of said figure

5 representation, every time a signal flowing in said
figure representation passes through said one of said
plurality of unit figures of said figure
representation.

22. The computer readable recording medium for
recording a program for a process according to Claim
21, wherein said signal includes a plurality of bits,
and

5 wherein said plurality of bits of said signal
are passed through said one of said plurality of unit
figures in parallel, and

wherein said (b) includes storing said point
allocated to said unit figure for each of said
10 plurality of bits, and

wherein said (c) includes giving said point for
each of said plurality of bits to said unit figure,
and

wherein said (d) includes outputting said point
15 for each of said plurality of bits given to said
figure representation.

23. The computer readable recording medium for
recording a program for a process according to Claim

09766675 012301

22, wherein said (d) includes calculating a mean value
of said points corresponding to said plurality of bits
5 given to said figure representation, to output.

24. The computer readable recording medium for
recording a program for a process according to Claim
16, further comprising:

(f) presenting said points outputted by said
5 (d) in graphical form.

25. The computer readable recording medium for
recording a program for a process according to Claim
24, wherein said (f) includes sorting said points
outputted by said (d) to present.

0976675 01301
FOE210 5299260